UNITED STATES OF AMERICA
BEFORE THE NATIONAL LABOR RELATIONS BOARD
DIVISION OF JUDGES

KAISER FOUNDATION HEALTH PLAN, INC.; KAISER FOUNDATION HOSPITALS; SOUTHERN CALIFORNIA PERMANENTE MEDICAL GROUP; AND THE PERMANENTE MEDICAL GROUP

Respondents

and **Case 32-CA-169979**

ENGINEERS AND SCIENTISTS OF CALIFORNIA, LOCAL 20 IFPTE, AFL-CIO/CLC,

Charging Party

RESPONDENTS' POST-HEARING BRIEF

MICHAEL R. LINDSAY
mlindsay@nixonpeabody.com
ALICIA C. ANDERSON
acanderson@nixonpeabody.com
MAE HAU
mhau@nixonpeabody.com
NIXON PEABODY LLP
300 South Grand Avenue, Suite 4100
Los Angeles, CA 90071
Telephone: (213) 629-6000
Fax: (213) 629-6001

APRIL L. WEAVER
april.l.weaver@kp.org
Kaiser Permanente Legal Department
One Kaiser Plaza, 19th Floor
Oakland, CA 94612

Attorneys for Respondents

Table of Contents

Page

Table of Contents

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES

Page(s)

TABLE OF AUTHORITIES

Page(s)

Statutes

TABLE OF AUTHORITIES

I. INTRODUCTION

The Region and Counsel for the General Counsel filed this case in an effort to expand the coverage of the National Labor Relations Board's (the "Board") decision in *Purple Communications*, 361 NLRB No. 126 (2014), *appeal filed*, No. 17-70948 (9th Cir. April 3, 2017) ("*Purple Communications*"), to include modalities of workplace electronic communications beyond email. After compelling respondents Kaiser Foundation Health Plan, Inc. ("KFHP"), Kaiser Foundation Hospitals ("KFH"), Southern California Permanente Medical Group ("SCPMG"), and The Permanente Medical Group ("TPMG") (collectively, "Respondents" or "Kaiser" or "KP") to produce thousands of pages of documents about Kaiser's electronic assets, their usage in the workplace and other matters, Counsel for the General Counsel abandoned that effort.

What was left was a challenge, albeit a half-hearted one (neither Charging Party nor Counsel for the General Counsel saw fit to present any witnesses at the hearing) to certain long term provisions of Respondents' Electronic Asset Usage National Policy (the "Electronic Asset Policy"). The rules contained within the Electronic Asset Policy are lawful and have been in effect for a number of years. The contrary arguments, if any, of Counsel for the General Counsel and Charging Party, Engineers and Scientists of California, Local 20 IFPTE, AFL-CIO/CLC ("Charging Party" or the "Union") are completely without merit, and the Complaint in this case should be dismissed.

In addition, the basis of the remaining provisions of the Complaint is an expansive reading of the decision in *Purple Communications.* As shown more fully below, that decision was contrary to long established Board and Court decisional law and should be overturned. This case presents the ideal vehicle for the Board to correct the errors of its prior decision.

The Union and the General Counsel assail individual provisions in Respondents' general employment policies designed to safeguard protected health information ("PHI"), prevent cyber security breaches, and comply with statutory prohibitions on unlawful recordings. None of these provisions individually, and certainly not when read in the context of the entire policies, violates

Section 8(a)(1) of the National Labor Relations Act ("Act"). Indeed, there is no allegation that such provisions explicitly restrict Section 7 activities (which they do not). Nor is there any allegation that Kaiser promulgated these rules in response to union activity (which they did not do). And there is no allegation that Kaiser ever applied the Electronic Asset Policy to restrict the exercise of Section 7 rights (which Respondents have not done).

Rather, the Union and the General Counsel argue – in a theoretical context entirely of their own making that – that Kaiser's mere maintenance of such policies violates Section 8(a)(1) because they could somehow be construed as prohibiting Section 7 activity. However, because Kaiser is a healthcare institution, it has strict obligations under the Health Insurance Portability and Accountability Act ("HIPAA") to protect PHI. Kaiser has adopted policies to further this objective – including a policy that restricts an email to 500 recipients and limits audio or visual recordings on its premises. Kaiser's policies also secure its internal email network from cyber-attacks, in order to systematically reduce the risk that this health care provider's computer systems will fall victim to hackers seeking a ransom payment or to obtain PHI for misuse. In this high-risk environment of on-going an active cyber-attacks on all of our institutions in the United States, health care providers are particularly susceptible to such attacks.

Under current Board law, the General Counsel bears an extremely heavy burden of proving that these facially neutral and critically important policies safeguarding patient privacy, protecting PHI, and protecting an email system used daily by nearly 200,000 employees somehow when read by a reasonable employee deter that employee from exercising Section 7 rights. Neither Counsel for the General Counsel nor the Charging Party presented any evidence on any employee being so deterred. Thus they must prove that the policies alone, taken as a whole (although they seek to challenge only specific portions of the policies), are so facially flawed as to violate Section 7 rights. Kaiser's narrowly-tailored policies are fully justified by the special circumstances of the health care industry and do not violate the Act.

II. STATEMENT OF FACTS

A. Kaiser And Its Electronic Asset Policy

Respondents are four distinct entities operating in the healthcare industry whose business is located primarily in California. (Tr. 82:12-15.) KFHP is the health plan organization that provides benefits to approximately 11.8 million of Kaiser patients, or "members." (Tr. 61:18-21.) KFH holds, manages, and maintains all of the hospital facilities. (Tr. 61:24-25.) KFHP and KFH are both nonprofit entities that operate inside and outside California. (Tr. 61:21-62:2.) Conversely, TPMG and SCPMG provide medical care to Kaiser members in California, and have employees only in California. (Tr. 62:2-10; 113:5-10.) Respondents collectively employ nearly 200,000 employees. (Tr. 148:11-14.)

The Electronic Asset Policy, which has been in effect in pertinent part since 2008, governs employees' use of Kaiser's electronic assets, including its computers, cell phones, and email systems, and which are made available for employee use during working hours. (Joint Ex. 1; Tr. 75:9-10.) The Electronic Asset Policy is available to employees on Kaiser's intranet. (Tr. 205:4-10.) Given Kaiser's size and complexity, its policies do not exist in isolation and are expressly linked to other policies. (Tr. 81:12-17.) This is true of the Electronic Asset Policy, which references several related policies that provide further information related to issues covered by the Electronic Asset Policy. (See e.g. GC Ex. 2 § 5.3.8 (referencing other policies that pertain to requirements on video recording patients, members, and staff).)

Respondents adopted the first version of the Electronic Asset Policy in February 2008. (Tr. 75:9-10.) Between 2008 and 2015, the policy had been revised five different times to address various issues and concerns.[1] ((Tr. 84:23-85:1; Respondents' Ex. 6.) Policy discussions

[1] At the hearing, the ALJ rejected Respondents' presentation of testimony and documentary evidence of the prior revisions of the policy except for the original 2008 version, including Respondents' proffer of the version of the policy dated January 10, 2013 (Respondents' Rejected Ex. 5) – which reflects the policy as it existed immediately prior to the 2015 revision – on grounds that the presentation of such evidence "would overburden the record." (Tr. 85:7-87:7; 87:14-88-9; 100:18-101:5.) Respondents believe that this evidentiary ruling was made in error and preserve their right to appeal to the extent that the ALJ's ruling handicapped their ability to present their defense in this matter – most notably to proffer an explanation, on a full record, of Respondents rationale for various drafting choices that explains the current language of the challenged subsections, much of which harkens back to prior

(Footnote continued on next page)

at Kaiser are helmed by its national human resources policy roundtable (the "HR Roundtable"), a cross-regional, cross-functional work group that is comprised of human resources professionals across Kaiser entities. (Tr. 71:4-6.) The HR Roundtable reviews, develops, and publishes national human resources policies for Kaiser's entire workforce. (Tr. 71:2-4; 71:23-72:4.) Although the HR Roundtable creates Kaiser's policies, these policies do not take effect until they are approved by the regional human resources leaders. (Tr. 92:11-95:8.)[2]

In August 2009, the Board's Division of Advice reviewed and expressly approved Kaiser's Electronic Asset Policy. *See Kaiser Permanente*, 37 NLRB AMR 73, No. 32-CA-24388 (2009). The Board found that the policy was facially valid and that Kaiser did not disparately enforce the policy against the alleged discriminatee.[3]

The latest version of the Electronic Asset Policy went into effect on January 1, 2015. (Tr. 98:20-99:2.) It was specifically revised in 2015 to comply with the Board's holding in *Purple Communications*, 361 NLRB No. 126 (2014), *appeal filed*, No. 17-70948 (9th Cir. April 3, 2017). (Tr. 96:15-24; 110:18-22; 111:7-9.) In Section 5.3.4 of the Policy, Kaiser added references to Section 7 of the Act to state that "this provision does not apply to communications made by employees during non-working time that are protected under Section 7 of the National

---

revisions. Additionally, to the extent that the General Counsel or the Charging Party attack the foundation of witness Derek Reimer's understanding of the policy language in 2015 as a means of discrediting his testimony, Respondents submit that they were unduly prevented from presenting a thorough history of his knowledge of the language that is subject to dispute by the ALJ's ruling preventing the presentation of this evidence. The ALJ cannot prevent Respondents' from presenting evidence that would have bolstered Mr. Reimer's foundation while simultaneously discrediting Mr. Reimer's testimony for lack of foundation.

[2] Derek Reimer testified that he participated in all but one of the revisions to the Electronic Asset Policy in his role as chair of the HR Roundtable from approximately 2004 to 2016. (Tr. 74:9-18.) He further testified that he is very familiar with the history associated with the development of the Electronic Asset Policy, including the 2015 revision during which time he had a brief hiatus from the roundtable, as he received all archival records from his predecessor when he reassumed responsibility as chair of the HR Roundtable in May 2016. (Tr. 74:19-23; 103:9-19.) Additionally, because the policy provisions that are at issue in this case have not significantly changed since 2008, Mr. Reimer's testimony about Respondents' intent in drafting these policies are highly relevant.

[3] At the hearing, Respondents requested that the ALJ take judicial notice of the charge, the Region's denial letter, and the Board's 2009 Advice Memorandum. (*See* Respondents' Ex. 7; Rejected Respondents' Exs. 7(A-C).) The ALJ denied judicial notice of these documents on grounds of relevance. (Tr. 212:15-215:13.) Respondents submit that the Board's prior review of the same policy at issue in this case is subject to mandatory judicial notice and is relevant to these proceedings. (*Id.*) Respondents preserve their rights to appeal this issue.

Labor Relations Act." (Tr. 96:8-14.) Additionally, to clarify that employees were permitted to discuss Section 7 protected subjects despite various restrictions within the policy pertaining to the protection of Confidential and Proprietary Information, revisions were made to the definition of Confidential and Proprietary Information to make clear that "Confidential information does not include information about wages, hours, benefits and other terms and conditions of employment." (GC Ex. 2 § 4.2; Tr. 88:17-89:5.) Kaiser also made minor modifications to the Personal Use Section, as described further below. In accordance with the Act, no employee has been disciplined, counseled, or warned for violating any provision of this latest Electronic Asset Policy. (Tr. 99:10-13.)

In this case, the General Counsel challenges two sections of the electronic asset policy: section 5.2 (the "Personal Use Section"), including two subsections, 5.2.1 (the "Incidental Use Subsection") and 5.2.2 (the "Mass Personal Messages Subsection"), and section 5.3.8 (the "Recording Section"). (GC Ex. 2.) The Personal Use Section is designed to allow for incidental *personal* use of Kaiser's electronic assets, including its email system, and at the same time forbids the sending of mass *personal* messages that are entirely unrelated to an employee's work at Kaiser. The Recording Section restricts employees from making audio, digital, and video recordings without obtaining consent of persons who are being recorded.

B. The Personal Use Section Of The Electronic Asset Policy

Kaiser recognized that employees will have personal activities that occur during working hours, and therefore designed the Personal Use Section to permit incidental, limited personal use of the company's electronic assets. (Tr. 89:24-90:6.) The term "Personal Use" is defined in the policy as the "[u]se of KP Electronic Assets that is for personal reasons that do not relate to an employee's work for KP or other issues relating to KP." (GC Ex. 2 § 4.5.) Thus, on the face of the policy, the "Personal Use" provisions do not apply to communications that have anything to do with the workplace, including Section 7-protected communications, and do not otherwise prohibit Section 7-protected communications. (*Id.*)

1. The Incidental Use Subsection of the Personal Use Section

Within the Personal Use Section, the Incidental Use Subsection addresses and limits the use of electronic assets for purely personal reasons that do not relate to the employee's work or issues related to the employee's work. The Incidental Use Subsection provides as follows:

> Personal Use of KP Electronic Assets, as defined in this policy, must be incidental, limited in frequency and scope, cannot incur additional costs to KP, and cannot impact employee performance.

(*See* GC Ex. 1 § 5.2.1.) Because the policy applies only to the "Personal Use" of electronic assets, by its terms, the simple provision does not in any way limit employees' use of electronic assets for Section 7-protected communications – it limits only their use of electronic assets for purely personal reasons. (*Id.*)

Since its inception in 2008, the Electronic Asset Policy has always included a Personal Use Section containing an Incidental Use Subsection. (Respondents' Ex. 1 (2008 Policy) § 5.4.1.2; Tr. 90:1-3.) Kaiser recognizes that employees have lives outside of work and that life activities frequently intervene during working hours. (Tr. 89:23-90:1.) The Incidental Use Subsection therefore permits incidental limited personal use of company assets as Kaiser does not pretend that this does not happen frequently or at all times. (Tr. 90:2-6.)

In 2015, the HR Roundtable made revisions to the policy to comply with *Purple Communications*. (Tr. 96:21-93:3.) The revisions included adding to the Electronic Asset Policy a definition of "Personal Use" as a defined term (as distinguished from "Working Time," which was also added as a defined term) and added the words "as defined in the policy" to the language of the Incidental Use Subsection. (GC Ex. 2 (2015 Policy) §§ 4.5, 4.6, 5.2.1; Tr. 89:6-19.) These changes made more clear that the Incidental Use Subsection applied *only* to the "Personal Use" of electronic assets, as defined in the policy. The remaining language in the Incidental Use Subsection remained unchanged from its prior iteration.

2. The Mass Personal Messages Subsection of the Personal Use Section

Also within the Personal Use Section, the Mass Personal Messages Subsection addresses and limits the sending of **personal** emails to a large number of recipients where there is no business need to do so. On its face, the Mass Personal Messages Subsection limits only the sending of mass **personal** messages having nothing to do with the workplace, and provides as follows:

> Employees should not send "mass" **personal messages** (sent to large numbers of recipients).[4] For example, employees may not use KP's Electronic Assets to initiate or forward chain letters, jokes, or other **personal mass mailings** that have no business purpose. Employees may only send authorized messages to large numbers of recipients when there is a clear business need to do so, and only as authorized by the appropriate KP manager.

(*See* GC Ex. 2 § 5.2 (emphasis added).)

Kaiser initially adopted a prohibition on employees from sending mass emails in 2008 to address the persistent, and continuing, problem of employees' use of company networks and email systems to forward email or chain letters to large numbers of recipients, which created an unnecessary drain on the employers' network systems. (Tr. 79:15-19; 84:17-22; 95:14-17; *see* Respondents Ex. 1 (2008 Policy) § 5.2.4.) In 2015, when the policy was revised to be consistent with *Purple Communications,* the mass email prohibition was moved from the section describing general prohibitions on the use of electronic assets to the "Personal Use" section, and language was added limiting the provision to mass **personal messages** only. (*Compare* Respondents' Ex. 1 (2008 Policy) § 5.2.4 *with* GC Ex. 2 (2015 Policy) § 5.2.2; Tr. 90:7-91:18.) These changes make clear that the Mass Personal Messages Subsection applies only to "Personal Use" of electronic assets.

The mere act of sending a "mass" email to thousands of users causes a significant performance hit on the email systems. (Tr. 137:9-138:10.) Naturally, the numerous recipients

[4] As described at the hearing, Kaiser defines a "mass" email as a single email addressed to 500 or more recipients, and builds these limitations into its email system functions. (Tr. 136:8-15; 137:24-25.) The policy and the technological limitations on the system thus permits emails addressed to 499 or fewer recipients. (Tr. 136:21-22.)

may be prompted to "reply all" to the entire recipient list. Even in the case of 100 to 200 recipients, responses to a mass email can cause technical issues. (*Id.*) Needless to say, these issues would multiply exponentially if the mass email was sent to all of Kaiser's employees—approximately 200,000 recipients. (Tr. 148:11-14; 161:1-9.)

Attachments to the mass emails, in varying file size and type, can further drain the technical and system resources, thus disrupting Kaiser's operations and impacting employees' ability to send and receive emails. (Tr. 79:20-24.) To illustrate this "bottleneck" effect, consider the scenario where an employee is traveling on an airplane, is using a cellphone to access email, or is otherwise in an area with a slow connection. Upon receiving a mass email with a large attachment, the employee would have no choice but to wait until the email message is fully downloaded—a process that can take significant time in these circumstances—until he or she can receive other work-related emails. (Tr. 138:11-20.) These issues are so prevalent that Kaiser information technology administrators have had to go to individuals directly to ask them to stop replying to the mass emails. (Tr. 162:22-25.)

By contrast to mass emails sent by individual employees, those sent by qualified Kaiser administrators pose less of an issue because they can configure email message settings to mitigate the undesired impact on system performance. (Tr. 150:1-18.) For instance, administrators can "blind copy" recipients, which means that recipients cannot simply click "reply all" to other recipients. (*Id.*) Administrators can also disable responses entirely to avoid the problem of users automatically responding and forwarding the mass email to even more recipients. (*Id.*) Ordinary employees who are unfamiliar with these settings options are less able to mitigate the impact of a mass email on the system. (*Id.*)

Restrictions on sending mass personal messages address another equally valid concern separate and apart from network integrity: Kaiser's need to put measures in place to protect against cyber security breach. (Tr. 128:20-23.) Such a breach occurs when an information technology asset (i.e. email) is used in an unintended manner, oftentimes to steal data or harm a computer network or system. (*Id.*) The presence of security measures such as limits on mass

emailing are crucial in preventing such attacks because 90 percent of cyber security breaches start with email "vector," or method of entry. (Tr. 129:1-3.) Kaiser receives more than 200 million messages every month from external sources, and 85-90% of those messages are discarded because they contain malicious content, or "malware." (Tr. 120:11-13; 130:13-16.) These attacks vary in sophistication and may contain malware in the messages themselves. Indeed these "phishing" attempts are carefully designed ploys to build trust with a Kaiser employee to convince them, among other things, to share their password(s) (Tr. 132:5-8), access a malicious link or file designed to infect the entire system (Tr. 132:14-19), or hold the user's files hostage until a "ransom" payment is made. (132:22-133:6.) These attacks have only increased in sophistication and frequency, and are far from hypothetical situations. In May 2017, National Health Services—the primary healthcare provider in the United Kingdom, fell victim to an email attack due to the very same "ransomware" described above, joining a long list of health care institutions that had similarly been targeted. (Tr. 142:10-24.)

Although Kaiser has in place several mechanisms for the screening and discarding of malicious emails from external services, due to technical logistics, operational necessity, and cost considerations, there are typically fewer safeguards when it comes to emails sent internally between Kaiser employees. (Tr. 134.6-16.) These internal emails are deemed "trusted" and subject to fewer controls in order to streamline ordinary day-to-day transmission of internal communications. (Tr. 135:20-25.) Thus, if mass emails were not limited, an attacker need only gain access to one employee's email account to quickly spread computer malware or viruses to hundreds of thousands of Kaiser employees simultaneously. (Tr. 137:9-138:10.)

Finally, the Mass Personal Messages Subsection is essential in preventing or mitigating the unauthorized disclosure of PHI, which includes information relating to a patient's personal identification, their medical records and conditions, and history or future health insurance details. (Tr. 170:3-9.) While Kaiser employees are extensively trained in maintaining the confidentiality of PHI, the ease and speed in which such information can be inadvertently sent or forwarded to hundreds, or even thousands, of employees presents a significant challenge to Kaiser's obligation

to protect such information. (Tr. 145:4-14). Healthcare institutions such as Kaiser are the number one targets for attackers because of the value of PHI on the dark web. (Tr. 139:23-140:2.) Attackers lock the network systems with ransomware and block access to patient information, thereby shutting down medical procedures. (Tr. 140:2-5.) It is not until the healthcare institution pays a ransom to the attackers are the networks restored. (Tr. 140: 6-8.) These threats have only increased, and have shut down hospitals such as MedStar, Hollywood Presbyterian, and the National Health Services in the United Kingdom. (Tr. 142:10-24.)

C. The Recording Section Of The Electronic Asset Policy

As with the Mass Personal Messages Subsection, the Recording Section of the Electronic Asset Policy safeguards PHI by ensuring that PHI is not, whether deliberately or accidentally, captured in a recording and then transmitted to others. (Tr. 82:2-5.) The Recording Section states that:

> Employees may not make audio, digital or video recordings on KP premises, or of KP personnel, patients or their family members, with personal or KP Electronic Assets, without the consent and authorization of all who are being recorded. Consent is implied or is not required in certain limited sitations, such as KP security system recordings and KP-authorized events (e.g., Town Hall events, executive leadership forums, KP compliance awareness fairs, retirement award celebrations, KP Thrive events).

(*See* GC Ex. 1 § 5.3.8.)

The language of the Recording Section was drafted in 2008. (Tr. 81:20-24; Respondents' Ex. 1 (2008 Policy) § 5.2.8.) It addresses the ubiquity of PHI throughout all of Kaiser's facilities. As discussed above, PHI includes any information related to individuals, their health, and their health insurance. (Tr. 170:3-9.) It is not limited to medical information, but encompasses identifying marks on an individual, such as a birth mark or tattoo. (Tr. 170:22-171:1; 171:4-9.) It is important to understand that the presence of PHI in a health care facility is not limited to so-called "immediate patient care areas," as that term has been used in Board law. PHI is located throughout the hospital setting; it is the patients themselves, what can observed of

the patients (e.g., whether they are on a gurney or intubated), discussions by caregivers about the patient, and information posted on walls about the patient (e.g., hospital charts or operating room schedules). (Tr. 171:17-25; 195:19-24; 196:2-10.) Given the breadth of PHI throughout the workplaces, the risk of inadvertently capturing such information by making recordings on Kaiser premises is substantial. (Tr. 179:14-18.)

Kaiser is legally bound to protect all such PHI under HIPAA, and is subject to fines and penalties for any violation. (Tr. 173:14-19.) Kaiser's obligation to protect PHI is also rooted in its contractual requirements with entities that purchase its health insurance, including employer groups that purchase insurance for its employees and governmental purchasers that provide coverage through Medicare, Medi-Cal, and state employee programs. (Tr. 173:1-6.) These contracts also impose penalties for violations. (Tr. 173:14-19.) In addition to fines, the Joint Commission for Healthcare Organizations and the National Committee on Quality Assurance may revoke Kaiser's accreditation or license for breaching its duty to safeguard PHI. (Tr. 174:1-7.)

Along with safeguarding PHI, Kaiser adopted the Recording Section to ensure a safe and secure work environment for employees, patients and their family members, as well as to prevent undue disruptions to the workplace posed by the recording of employees, patients, and their family members without their knowledge. (Tr. 82:7-11.) The Recording Section also was enacted to comply with California state law, as well as the laws of other states that have similar provisions, that prohibit the recording of confidential communications without the consent of all parties to the conversation. (Tr. 82:12-15.) Kaiser, which is primarily located in California, did "not want to express anything in its policy that would intentionally violate [California] law." (Tr. 82:15-17.) Apart from minor clarifications, the first sentence of the Recording Section – i.e., the sentence that prohibits employees from making "audio, digital or video recording on KP premises, or of KP personnel, patients or their family members" without consent – has remained

largely unchanged since it was first drafted in 2008.[5] (*Compare* Respondents' Ex. 1 (2008 Policy) § 5.2.8 *with* GC Ex. 2 (2015 Policy) § 5.3.8; Tr. 82:18-83:7.)

D. The General Counsel Presented No Evidence That Kaiser, Or Any Employee Of Kaiser, Ever Interpreted The Electronic Asset Policy To Prohibit Section 7 Activity

There is no evidence in the record, nor does the General Counsel contend, that Kaiser promulgated the Electronic Asset Policy in response to union activity or has applied the Electronic Asset Policy to restrict Section 7 rights. There is also no evidence that the policies have chilled union speech. The General Counsel and the Union did not present any evidence or witnesses at the hearing to show that employees would reasonably construe the Electronic Asset Policy to chill their Section 7 rights. Indeed Kaiser has not disciplined, counseled, or warned any employee for violating any provision of the Electronic Asset Policy. (Tr. 99:10-13.) Nor did the General Counsel present any witnesses in rebuttal to Kaiser's witnesses. Accordingly, there was no contrary evidence presented and no need for any credibility findings to be made.

III. LEGAL STANDARD & BURDEN OF PROOF

On an 8(a)(1) claim, the General Counsel carries the burden of "showing that the maintenance of [a] rule would reasonably chill employees in the exercise of their Section 7 rights." *Lafayette Park Hotel*, 326 NLRB 824, 826 (1998). The Board must dismiss the complaint if it finds that the General Counsel has failed to meet its burden. However, if the General Counsel establishes that the employer's policy adversely affects employees' protected rights, then the burden shifts to the employer to demonstrate "legal and substantial business justifications" for its conduct. *Jeannette Corp. v. NLRB*, 532 F.2d 916, 918 (3d Cir. 1976) (citation omitted).

Consistent with the foregoing, the inquiry into whether the employer's maintenance of a challenged rule unlawfully chills an employee's Section 7 rights begins with the issue of whether

[5] A second sentence was added in 2008 or 2009 to address some confusion in the organization with respect to the recording by the organization of Kaiser-sponsored events where employees could be present. (Tr. 83:8-24.) However, this part of the Recording Section does not appear to be challenged in this proceeding.

the rule *explicitly* restricts activities protected by Section 7. *Lutheran Heritage Village-Livonia,* 343 NLRB 646, 646 (2004). If the rule restricts Section 7 activities on its face, the Board will find the rule unlawful. *Id.* at 646 & n.5 (for example, a rule that explicitly prohibits an employee activity that the Board has repeatedly found to be protected by Section 7 would be considered unlawful on its face). If the rule does not explicitly restrict activity protected by Section 7, the violation is dependent upon a showing of one of the following: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights. *Id.* at 647.

In assessing a claimed violation, the challenged rule must be given a "reasonable reading." *Id.* at 646-47. The Board must refrain from reading particular phrases in isolation because "limiting language can narrow the scope of a rule so that it does not infringe on the exercise of Section 7 rights." *Copper River Grill*, 360 NLRB No. 60, at 23 (2014) ("[L]anguage in a rule which relates a prohibition to a specific legitimate business purpose may well affect how employees reasonably understand the scope of the rule."); *Lafayette Park*, 326 NLRB at 825 (the General Counsel may not "pars[e] the language of the rule" in hopes of extracting a violation), *enforced* 203 F.3d 52 (D.C. Cir. 1999). Moreover, the Board "must not presume improper interference with employee rights," *Copper River*, 360 NLRB No. 60 at 13 (quoting *Lutheran Heritage*, 343 NLRB at 646), and it may not speculate whether a rule improperly intrudes upon Section 7 rights, *see Cox Commc'ns, Inc.*, Case No. 17- CA-087612 (Div. of Advice, Oct. 19, 2012) ("The Board will not find a violation simply because a rule could conceivably be read to restrict Section 7 activity."). Instead, a rule may be found unlawful only if – when reasonably read in context – it is "***likely*** to have a chilling effect." *Lafayette Park*, 326 NLRB at 825 (emphasis added).

The General Counsel did not carry its initial burden here. The General Counsel presented no evidence beyond the Electronic Asset Policy itself, but the policy does not explicitly prohibit Section 7 activity. In addition, there is no contention nor did the General Counsel present any

evidence that the rule was promulgated in response to union activity or that the rule has been applied to restrict the exercise of Section 7 rights. Instead, the General Counsel has ignored the Board's direction to give the policy a reasonable reading and challenges three *subsections* of the Electronic Asset Policy, trying to isolate these subsections from the rest of the policy to assert its case. But when the entire Electronic Asset Policy is read together, and absent any actual evidence supporting its allegation that employees would reasonably construe the language of the policy to prohibit Section 7 activity, it becomes apparent that the General Counsel has utterly failed to meet its initial burden.

Presuming, *arguendo*, that the General Counsel had met its initial burden and shifted to Kaiser the burden of showing legal and substantial business justifications for the policies, the case should still be dismissed. The email restrictions at issue in this case are consistent with recognized limitations an employer may place on employees' personal use of an employer's email system. The video recording restrictions are entirely consistent with restrictions allowed for a healthcare employer as recognized in *Flagstaff Medical Center,* 357 NLRB No. 65 (2011) and *Whole Foods,* 363 NLRB No. 87 (2015). Under these standards, the Electronic Asset Policy's provisions at issue in this case are lawful, and the Complaint should be dismissed in its entirety.

IV. ANALYSIS

A. The Charge Against Health Plan, Hospitals And SCPMG Is Untimely

Section 10(b) of the Act disallows the issuance of complaints "based upon any unfair labor practice occurring more than six months prior to the filing of the charge with the Board and the service of a copy thereof upon" the charged party. 29 U.S.C. § 160(b). The 10(b) period begins to run when the aggrieved party has "clear and unequivocal notice of a violation." *Leach Corp.*, 312 NLRB 990, 991-92 (1993), *enforced* 54 F.3d 802 (D.C. Cir. 1995). Knowledge is imputed when the aggrieved party first has "knowledge of the facts necessary to support a ripe unfair labor practice." *Castle Hill Health Care Ctr.*, 355 NLRB 1156, 1191 (2010); *see also St. Barnabas Medical Ctr.*, 343 NLRB 1125, 1127 (2004).

The Complaint in this matter stems from a charge filed by the Union against TPMG **only** on February 18, 2016,[6] alleging that the Electronic Asset Policy violated the Act. The Union was placed on notice of the revisions to and promulgation of those policies by TPMG, KFH, KFHP, and SCPMG **at the same time**. By its terms, the Electronic Asset Policy applies to ***all*** of these entities. Thus, the Union had actual knowledge at the time it filed the original charge against TPMG that the Mass Email Policy and the Recording Policy also applied to the other respondents. *See Miramar Hotel Corp.*, 336 NLRB 1203, 1252 (2001) (if a party "ha[s] the means of discovery [of a fact] in his power, he will be held to have known it" and "whatever is notice enough to excite attention and put the party on his guard and call for inquiry, is notice of every thing to which such inquiry might have led") (quotations and citation omitted here and throughout). Notwithstanding the policies' clear language, the Union elected to name **only** TPMG in the original charge.

On October 20, 2016, eight months after the original charge was filed, and well after the six-month limitations period had fully expired, the Union amended its charge to name the additional respondents. Thus, the Union's charge against all parties except TPMG was untimely, and should be dismissed.

The Union's amended Charge did not cure its error in failing to name all Respondents because the proposed amendment could not "relate back" to the original charge. Unfair labor practice proceedings, so far as practicable, look to the rules of civil procedure for the district courts of the United States. 29 U.S.C. § 160(b). Federal Rule of Civil Procedure 15(c), which otherwise allows certain amendments to relate back to an original complaint, only applies when a plaintiff is correcting a *mistake* in the original pleading, and not when belatedly adding a new party. *See Jordan v. Tapper*, 143 F.R.D. 567, 573-74 (D. N.J. 1992) ("[U]nder the rule, for a plaintiff to amend his complaint to add a new defendant, the plaintiff may not merely have failed

[6] Although the Union likely learned of the policy before, a formal letter was sent to the Union notifying it of the adoption of the policy on August 21, 2015.

to sue the proposed party; rather the plaintiff must have initially sued the wrong party and is attempting to correct the mistake."); *Bensel v. Allied Pilots Ass'n*, 387 F.3d 298, 309-10 (3d Cir. 2012) (in charge against union, court determined that plaintiff must satisfy Rule 15(c) for amended pleading to relate back to original charge). Or more directly, "an amendment which adds a new party creates a new cause of action and there is no relation back to the original filing for purposes of limitations." *Asher v. Unarco Material Handling, Inc.*, 596 F.3d 313, 318 (6th Cir. 2010).

Rule 15 only works to relate the addition of a new party back to an original complaint if that new party "knew or should have known that the action would have been brought against it, but for a mistake concerning the proper party's identity." Fed. R. Civ. P. 15(c). The rule is designed to protect a plaintiff who mistakenly targets the wrong defendant but later discovers the identity of the proper party. *G.F. Co. v. Pan Ocean Shipping Co.*, 23 F.3d 1498, 1503 (9th Cir. 1994). There was no mistake here. The Union chose to file its original charge against only TPMG, and not any of the other respondents, even though the policies on which the Union based its claims expressly state that they apply to all employees of TPMG, KFH, KFHP, and SCPMG. As the Supreme Court has held in connection with a similar case, under Federal Rule of Civil Procedure 15, where a plaintiff chooses to sue a certain defendant, and not others, with full understanding of the facts, the plaintiff cannot join the unnamed defendants after the statute of limitations has run. *Krupski v. Costa Crociere S. p. A.*, 560 U.S. 538, 552 (2010) ("When the original complaint and the plaintiffs conduct compel the conclusion that the failure to name the prospective defendant in the original complaint was the result of a fully informed decision as opposed to a mistake concerning the proper defendant's identity, the requirements of Rule 15(c)(1)(C)(ii) are not met."); *see also Louisiana-Pacific Corp. v. ASARCO, Inc.*, 5 F.3d 431, 434-35 (9th Cir. 1993) (no amendment allowed where no mistake of identity but conscious choice of whom to sue); *Kilkenny v. Arco Marine, Inc.*, 800 F.2d 853, 857-58 (9th Cir. 1986) ("Rule 15(c) was never intended to assist a plaintiff who ignores or fails to respond in a reasonable fashion to notice of a potential party, nor was it intended to permit a plaintiff to

engage in piecemeal litigation."); *In re Brocade Commc'ns Sys., Inc. Derivative Litig.*, 615 F. Supp. 2d 1018, 1041 (N.D. Cal. 2009) ("if a plaintiff is aware of the potential defendant's identity at the time the original complaint is filed, but is uncertain whether the potential defendant may be found liable, amendment is not allowed to defeat the statute of limitations"); *Hogan v. Fischer*, 738 F.3d 509, 517-18 (2d Cir. 2013) (noting that failing to identify an individual defendant is not a mistake for Rule 15(c) purposes); *Briggs v. Cty. of Monroe*, 09-CV-6147W3, 2016 WL 1296060, at *9 (W.D.N.Y. Mar. 29, 2016) ("Plaintiffs' proposed addition of the new defendants in this case does not seek to cure any mistake of identity; rather, it seeks to cure plaintiffs' ignorance of the potential culpability of the proposed defendants. That it does so after the expiration of the statute of limitations is fatal....").

In connection with pre-hearing discovery in this matter, Respondents raised similar arguments that the charges against Respondents other than TPMG were untimely.[7] (GC Ex. 1(k-l).) On July 6, 2017, the Administrative Law Judge ("ALJ") issued an order granting in part and denying in part Respondents' Petitions to Revoke ("Petitions"). (GC Ex. 1(n)("Order").) In the Order, the ALJ denied Respondents' Petitions based on Respondents' objection that the Union's charge was untimely "primarily for the reasons and authorities stated in the General Counsel's Opposition." (*Id.* at 3.)

Respondents object to the ALJ's adoption of the General Counsels' arguments and reaffirm their position that the amended charge against Respondents other than TPMG was untimely. The General Counsel's Opposition primarily relied on its erroneous argument that Respondents' 10(b) defense is inapplicable to because the Union alleges that Electronic Asset Policy was "maintained" during the 10(b) period (i.e. a "continuous violation" theory). (GC Ex. 1 (m) at 4.) The relevant case law, however, makes clear that the "continuing violation"

[7] On or about June 22, 2017, the General Counsel served separate subpoenas duces tecum on each respondent entity, TPMG (B-1-X39SZN), KFH (B-1-X45NI3), KFHP (B-1-X46IIH) and SCPMG (B-1-X47EV7) (collectively, the "Subpoenas"). On June 29, 2017, Respondents filed Petitions to Revoke four subpoenas duces tecum issued by the General Counsel. (GC Ex. 1 (k-l).) On July 5, 2017, the General Counsel filed an Opposition to Respondents' Petitions to Revoke. (GC Ex. 1 (m).)

exception to the six month statute of limitations proscribed by section 10(b) applies only where the policy is "invalid on its face." *See,* e.g. *Teamsters Local 293 (Lipton Distrib.)* 311 NLRB 538, 539 & n.2 (1993); *Great Lakes Carbon Corp.,* 152 NLRB 988, 989-90 (1965), *enforced* 360 F.2d 19 (4th Cir. 1966). Where, as here, a policy is not facially invalid, the policy may only be challenged when it was enacted within the statute of limitations or when an unlawful enforcement of the policy occurs within the statute of limitations. See *Local Lodge No. 1424 v. NLRB*, 362 U.S. 411, 419-420 (1960). Thus, as an initial matter, the complaint should be dismissed against all Respondents except TPMG on grounds that the amended charge was untimely.[8]

B. The General Counsel Fails To Meet Its Burden Of Proving That The Electronic Asset Policy Would Chill Employees' Exercise Of Section 7 Rights

1. The General Counsel misconstrues and fails to carry the General Counsel's initial burden

The General Counsel here misconstrues its initial burden of proving that the Electronic Asset Policy would reasonably chill employees in the exercise of their Section 7 rights. In its opening statement, the General Counsel stated, incorrectly, that the issues presented by this case are whether Respondents can establish special circumstances to justify the controls over its email

[8] Nor is the Board's decision in *Redd-I, Inc.*, 290 NLRB 1115 (1988), which stands for the proposition that "closely related" amendments to a charge relate back to the initial 10(b) period, dispositive here. *Redd-I, Inc.* relates only to an amendment that adds new **allegations** against existing parties, and does not address the issue of an amendment that adds new **parties**. Here, the amended charge does not meet the Board's test because there was no timely charge pending against all respondents when the Union amended its Charge. Instead, the original charge asserted a claim only against TPMG. Furthermore, the United States Supreme Court's decisions in *Ledbetter v. Goodyear Tire & Rubber Co.*, 550 U.S. 618 (2007), and *National Railroad Passenger Corporation v. Morgan*, 536 U.S. 101 (2002), has called into question the viability of the Board's test as stated in *Redd-I.* In *Ledbetter* and *Morgan*, the courts indicated that a "single wrong" perpetrated through a succession of acts (i.e., a series of actionable wrongs) is chargeable as long as some of the acts are within the limitations period. *See Morgan*, 536 U.S. at 115. A "discrete practices" claim, on the other hand, can avoid dismissal only if it alleges a specific act which occurred within the statutory period. *Ledbetter*, 550 U.S. at 639. Such "discrete practices" refer to a single occurrence, at a specific point in time, which is "independently identifiable and actionable." *Id.* When the Board in *Redd-I* analyzed whether the petitioner could amend the original charge to include an allegation of another employee's discharge, the Board mistakenly applied the Act's "single wrong" counterpart to allegations that are "independently identifiable and actionable." *See id.* Indeed, the situation did not fall into the "single wrong" category because each firing is an "independently identifiable and actionable" act. *See id.* The Board, in ruling that the complaint could be amended to include untimely allegations of an employee's discharge, ignored Supreme Court reasoning and allowed the plaintiffs to circumvent the Act's statute of limitations.

system, and whether these controls are necessary to maintain production and discipline. (Tr. 56:19-24.) The General Counsel's opening statement simply assumed an essential element of its case that it was required to prove. Where, as here, the policy does not explicitly prohibit Section 7 activity, it is the General Counsel's burden to show that employees would construe the Electronic Asset Policy as impacting any activity arguably protected by Section 7, and in fact presented ***no evidence*** beyond the policy itself to meet this burden. *See, Lutheran Heritage,* 343 NLRB at 646-47; *Caesars Entertainment*, Case 28-CA-60841, 2012 WL 949502 (2012) ("the Acting General Counsel had the burden of establishing by a preponderance of the evidence that employees would reasonably construe the computer usage rule to prohibit Section 7 activity"). The General Counsel offered no witnesses at the hearing and offered no evidence to establish that the Electronic Asset Policy had a chilling effect on Section 7 activity or that it was otherwise given an unlawful reading by Kaiser to stifle Section 7 activity.[9] In fact, the record shows that Kaiser has not disciplined, counseled, or warned any employee for violating any provision of the Electronic Asset Policy. (Tr. 99:10-13.) Where the General Counsel fails to meet its initial burden, Kaiser has no obligation to demonstrate that special circumstances are necessary for its Electronic Asset Policy. *See Lafayette Park Hotel*, 326 NLRB at 826 (dismissing complaint where "General Counsel has not met his burden of showing that the maintenance of this rule would reasonably chill employees in the exercise of their Section 7 rights).

[9] In 2010, and again in 2012, Respondents oversaw two statewide elections involving approximately 50,000 employees working at more than 1,000 facilities throughout California. These were arguably among the largest Board supervised elections in the history of the NLRB. As a month-long evidentiary hearing held under the auspices of Region 32 amply attested, the employees engaged in an unprecedented amount of Section 7 activity during the elections, and Respondents were not found to have violated the employees' rights in any way. Kaiser Foundation Health Plan, Inc. (National Union of Healthcare Workers), Case 32-RC-5775, Administrative Law Judge Report and Recommendations on Objections (July 14, 2011), *available at* http://apps.nlrb.gov/link/document.aspx/09031d458055a9cb. Moreover, during the election campaigns, Region 32, under the direction of the Division of Advice, *dismissed a charge which broadly challenged Respondents' Electronic Asset Policy. Kaiser Permanente*, 37 NLRB AMR 73, No. 32-CA-24388 (2009). Since that charge was dismissed, the Electronic Asset Policy has been amended for the sole purpose of adding broader and more explicit protections for Section 7 rights of employees. This background makes it particularly unwarranted to conclude without any supporting evidence that the Policy would be reasonably construed by employees to prohibit Section 7 activity.

2. A "reasonable reading" of the Electronic Asset Policy makes clear that the challenged provisions do not prohibit employees from engaging in Section 7-protected activity

In challenging the Electronic Asset Policy, the General Counsel improperly singles out specific subsections that it claims would chill Section 7 activity. However, Board precedent mandates that the challenged policy or work rule be given a "reasonable reading" and that the Board refrain from reading particular phrases in isolation because "limiting language can narrow the scope of a rule so that it does not infringe on the exercise of Section 7 rights." *Copper River*, 360 NLRB No. 60 at 13 (2014) ("[L]anguage in a rule which relates a prohibition to a specific legitimate business purpose may well affect how employees reasonably understand the scope of the rule."); *Lafayette Park*, 326 NLRB at 825 (1998) (the General Counsel may not "pars[e] the language of the rule" in hopes of extracting a violation), *enforced* 203 F.3d 52 (D.C. Cir. 1999); *Aroostook Cty. Reg'l Ophthalmology Ctr. v. NLRB*, 81 F.3d 209, 213 (D.C. Cir. 1996) ("In the absence of any evidence that [the employer] is imposing an unreasonably broad interpretation of the rule upon employees, the Board's determination to the contrary is unjustified.").

The Electronic Asset Policy, which encompasses several sections and subsections, is written and intended be read as a whole. (Tr. 81:12-17.) As a whole, the policy broadly governs the use of all electronic media and computing systems and devices provided by an employer in the healthcare industry, including but not limited to email, computers, cell phones and other mobile devices. (GC Ex. 2 § 4.3.) The policy describes the "Appropriate Use" of electronic assets, principally to perform job duties and other authorized activity relating to job functions. (*Id.* § 5.1.) The policy also describes "Prohibited Use" of electronic assets (*Id.* § 5.3), discusses the issuance of electronic assets (*Id.* § 5.4) and notifies employees of their obligation to immediately report lost, stolen or damaged electronic asset (*Id.* § 5.7), among other provisions. The context of the policy as a whole and its overarching purpose must be understood when reading the policy's provisions. Moreover, the Electronic Asset Policy specifically references several other policies that bear upon provisions within the policy, none of which were investigated by the General Counsel. (*See, e.g., id.* §§ 5.3.8 and 6.0.)

One of the sections of the Electronic Asset Policy that the General Counsel takes issue with addresses the "Personal Use" of KP electronic assets, with "Personal Use" defined by the policy to have a limited and specific meaning that does not include "an employees work for KP or other issues relating to KP." (*Id.* § 4.5, 5.2.) But other provisions within the Electronic Asset Policy that more directly apply to Section 7 communications expressly allow for Section 7 activity. For example, another section of the policy describes "Prohibited Use" of KP electronic assets. (*Id.* § 5.3.) The prohibited use section includes a prohibition on employee solicitation for outside organizations, but makes clear that Section 7 activity is protected.[10] (*Id.* § 5.3.4 (stating that the "provision does not apply to communications made by employees during non-working time that are protected under Section 7 of the National Labor Relations Act.") Additionally, although the policy restricts the unauthorized distribution of Confidential and Proprietary Information, the definition of "Confidential and Proprietary Information" specifically excludes information protected by Section 7, i.e. "wages, hours, benefits, and other terms and conditions of employment." (*Id.* § 4.2.) Because other provisions of the policy specifically allow for Section 7 protected activity, a holistic reading of the Electronic Asset Policy – rather than a reading of the challenged subsections in isolation – makes clear that employees would not understand the "Personal Use" restrictions to chill their Section 7 rights.

C. The Personal Use Section Does Not Violate Purple Communications

1. *Purple Communications* created only a limited right to use of an employer's email system for Section 7-protected activity

In *Purple Communications*, a 3-2 majority of the Board overruled *Register-Guard*'s holding that an employer could "lawfully bar employees' nonwork-related use of its e-mail systems." *Register-Guard*, 351 NLRB 1110, 1116 (2007), *remanded on other grounds*, 571 F.3d

[10] Notably, the "total ban" on nonbusiness use of the employer's email system that the *Purple Communications* majority found so offensive to the Act was a non-solicitation provision very much like Section 5.3.4, but that did not contain the carve-out for Section 7-protected activities like the one that appears in Kaiser's policy. Amongst other changes, Kaiser added the Section 7 carve-out to this provision specifically to comply with *Purple Communications*. The General Counsel does not take issue with this provision; rather, the General Counsel is concerned with the Personal Use provision as it relates to employee use of company email.

53 (D.C. Cir. 2009). Over two vigorous dissents, the bare majority of the Board in *Purple Communications* "presume[d] that employees who have rightful access to their employer's email system in the course of their work have a right to use the email system to engage in Section 7-protected communications on nonworking time." 361 NLRB No. 126 at 14.[11] Notably, the majority stated that its decision "do[es] not prevent an employer from establishing uniform and consistently enforced restrictions, such as prohibiting large attachments or audio/video segments, if the employer can demonstrate that they would interfere with the email system's efficient functioning." *Id.* However, apart from this statement, the *Purple Communications* majority did not declare any particular work rule invalid, nor has the Board addressed the application of the majority's newfound, presumed right in subsequent cases. *Id.* at 17 ("remand[ing] this aspect of this case...for further proceedings consistent with this decision"); *see also Purple Communications,* 365 NLRB No. 50, at *3 (Supplemental Decision and Order, March 24, 2017) ("*Purple Communications II*").

The "limited" right that the majority created in *Purple Communications* provides only that employees who otherwise have access to an employer's email system may use that system for Section 7-protected communications during non-working time. *See* 361 NLRB No. 126 at 14. Specifically, if the employer (1) grants employees access to the company email system in the course of their work and (2) maintains a prohibition on nonbusiness use of the company email system that is broad enough to encompass employees' use of the email system for Section 7 activities during nonworking time, this prohibition presumptively interferes with employees' Section 7 rights and violates Section 8(a)(1) of the Act unless the respondent rebuts that presumption by showing that the restrictions are justified by special circumstances necessary to maintain production or discipline. *Purple Communications II,* 365 NLRB No. 50 at *4.

[11] The viability of *Purple Communications* is in doubt. An appeal is presently pending in the Ninth Circuit, and the decision has received widespread criticism in the legal community. *See* 361 NLRB No. 126 (2014), *appeal filed,* No. 17-70948 (9th Cir. April 3, 2017).

Here, as described further below, the email restrictions imposed by the Electronic Asset Policy were drafted to specifically comply with *Purple Communications* and do not place any unlawful restrictions on employees' Section 7 protected use of the employer's email system. Indeed, the Personal Use Section challenged by the General Counsel with respect to access to company email applies only to "personal use" of the employer's email system and does not encompass employees' use of the email system for Section 7 activities; furthermore, other provisions of the policy specifically contemplates and allows for Section 7 protected communications where an explicit statement was needed to comply with *Purple Communications*. (See GC Ex. 2 § 5.3.4 (non-solicitation prohibition does not apply to "communications made by employees during non-working time that are protected under Section 7 of the National Labor Relations Act").)

Thus, the Electronic Asset Policy cannot presumptively interfere with employees' Section 7 rights, and there is no evidence that employees would construe the Electronic Asset Policy as impacting any activity arguably protected by Section 7. Regardless, the restrictions imposed by the Electronic Asset Policy, as they pertain to email use, is the type of restriction contemplated with approval by the *Purple Communications* majority.

2. The Email Restrictions Challenged By The Board Apply Only To The Narrowly Defined "Personal Use" of Electronic Assets; Section 7-Protected Communications Are Specifically Authorized Under the Policy

In this proceeding, the General Counsel challenges two subsections of the Electronic Asset Policy regarding email use, both set forth in the Personal Use Section (5.2) of the policy: the Incidental Use Subsection (5.2.1) and the Mass Personal Messages Subsection (5.2.2). However, the General Counsel's reading of the policy ignores the other key provisions in the Policy that make clear that the entirety of the Personal Use Section, including both the Incidental Use Subsection and the Mass Personal Messages Subsection, does not apply to Section 7-protected communications.

The two email use provisions challenged by the General Counsel both appear in the Personal Use section of the policy. (See GC Ex. 2 § 5.2.) "Personal Use" is a defined term in the policy, and therefore its usage throughout the policy has a specific meaning. As set forth in section 4.5, "Personal Use" is defined as:

> **Personal Use** – Use of KP Electronic Assets that is for personal reasons that **do not relate to an employee's work for KP** or other issues relating to KP.

(*Id.* § 4.5 (emphasis added).) Personal Use is distinguished from "Working Time," which is separately defined in the policy as:

> **Working Time** – Time during which an employee is required or scheduled to be on duty, exclusive of break time, meal time, or time before and after required or scheduled work time.

(*Id.* § 4.6.)

The definition of Personal Use and the distinction between Personal Use and Working Time make clear that the email provision at issue in this case, section 5.2, which governs only the "Personal Use of KP Electronic Assets," applies *only* to employees' use of electronic assets for "personal reasons that do not relate to an employee's work for KP or other issues relating to KP." Thus, the entire "Personal Use" section that is at issue in this case does not apply to an employee's use of the email system for Section 7 protected communications.

This interpretation is further reinforced by the language of the two subsections within the Personal Use Section. The Incidental Use Subsection (*Id.* § 5.2.1) states: "Personal Use of KP Electronic Assets, as defined in this policy, must be incidental, limited in frequency and scope, cannot incur additional costs to KP, and cannot impact employee performance." Again, "Personal Use" is a defined term within the policy, is capitalized when it appears in subsection 5.2.1, and has specific meaning – i.e. use for personal reasons "that do not relate to an employee's work for KP or other issues relating to KP." (*Id.* § 4.5.) Similarly, the language of the Mass Email Subsection (*Id.* § 5.2.2) makes clear that its prohibition is directed to personal use only: "Employees should not send 'mass' personal messages (sent to large numbers of

recipients). For example, employees may not use KP's Electronic Assets to initiate or forward chain letters, jokes, or other personal mass mailings that have no business purpose. Employees may only send authorized messages to large numbers of recipients when there is a clear business need to do so, and only as authorized by the appropriate KP manager."

Section 7 does not protect communications that are purely personal in nature and do not relate to an employee's terms and conditions of employment. *See Cellco P'ship*, 365 NLRB No. 38 (2017) (Section 7 protects employees' "communicat[ions] with each other regarding their workplace terms and conditions of employment"); *Karl Knauz Motors, Inc.,* 358 NLRB 1754, 1758 (2012) (Board adopting ALJ's finding that employee's Facebook posts of a Land Rover in a pond are "so obviously unprotected" because they that had no connection to any of the employees' terms and conditions of employment). Accordingly, *Purple Communications* only requires that employees be afforded the "right to use the [employer's] email system to engage in Section 7-protected communications" – i.e. communications that relate to an employee's terms and conditions of employment – "on nonworking time." 361 NLRB No. 126 at 14. Neither *Purple Communications* nor Section 7 requires that employees be afforded the right to use the employer's email system to engage in communications of a purely personal nature.

Because the Personal Use Section of the Electronic Asset Policy applies only to an employee's "Personal Use" of the email system, and because communications that "relate to an employee's work for KP" are specifically excluded from the policy's definition of "Personal Use," the Personal Use Section does not concern communications that are protected under the Act. Instead, a different section of the policy – a section that is notably ***not challenged*** by the General Counsel in this case – describes a prohibition on communications that could trigger protection under the Act, and explicitly carves out Section 7 protected communications. Specifically, section 5.3 of the Electronic Asset Policy describes the "Prohibited Use" of electronic assets, including email, without any constraints as to "Personal Use." Subsection 5.3.4 addresses solicitation and proselytization for outside organizations. Because this type of communication could be interpreted as prohibiting union organizing or other Section 7 protected

speech, Kaiser specifically added a disclaimer designed to comply with *Purple Communications*: "This provision does not apply to communications made by employees during non-working time that are protected under Section 7 of the National Labor Relations Act." Similarly, subsection 5.3.7 prohibits the dissemination of "Confidential or Proprietary Information (as defined in the policy)." "Confidential and Proprietary Information" is a defined term in the policy, set forth in section 4.2, and contains another specific disclaimer designed to carve out information protected by the Act that employees have a Section 7-protected right to share, such as information regarding wages, hours and working conditions: "**Note**: Confidential information does not include information about wages, hours, benefits, and other terms and conditions of employment."

3. The Electronic Asset Policy Was Specifically Revised to Comply With Purple Communications

Following the Board's issuance of the *Purple Communications* decision in December 2014, the Electronic Asset Policy was revised in 2015 with the specific intent to revise the policy in compliance with *Purple Communications.*[12] (Tr. 96:15-24; 110:18-22; 111:7-9.)

In *Purple Communications*, the majority of the Board examined an electronic communication policy that amounted to a total ban on all nonbusiness use of the employer's email system. 361 NLRB No. 126 at 3. Of note, not only was all email access limited to "business purposes only," but the employer also maintained non-solicitation provision that prohibited employees from engaging in activities on behalf of organizations or persons with no professional or business affiliation with the Company. The policy also prohibited employees

[12] Between 2008 and 2015, the policy had been revised five different times to address various issues and concerns. (Tr. 84:23-85:1.) At the hearing, the ALJ rejected Respondents' presentation of testimony and documentary evidence of the prior revisions of the policy except for the original 2008 version, including Respondents' proffer of the policy as it existed immediately prior to the 2015 revision, on grounds that such evidence would "overburden the record." (Tr. 87:14-88-9; 100:18-101:5.) Respondents believe that this evidentiary ruling was made in error and preserve their right to appeal to the extent that the ALJ's ruling handicapped their ability to present their defense in this matter – most notably to proffer an explanation, on a full record, of Respondents rationale for various drafting choices that explains the current language of the challenged subsections, much of which harkens back to prior revisions.

from sending "uninvited email of a personal nature." All of these provisions of the employer's email system were called out in the majority opinion in *Purple Communications. Id.* However, the Board also recognized that, "employers may nonetheless apply uniform and consistently enforced controls over their email systems to the extent that such controls are necessary to maintain production and discipline." *Id.* at 14.

When the Electronic Asset Policy was revised in 2015 to comply with *Purple Communications,* the most obvious changes that needed to be made were to sections in which an explicit carve out for Section 7 communications would need to be added to allow for Section 7 protected use of the email systems where previously Section 7 use was prohibited. For example, consistent with the Board's prior precedent in *Register Guard,* the policy previously contained a non-solicitation policy that prohibited using company electronic assets, including email systems, for solicitation for outside organizations. (Respondents' Ex. 1 (2008 Policy) § 5.2.1.) Thus, language was added to the non-solicitation provision to make clear that the "provision did not apply to communications made by employees during non-working time that are protected under Section 7 of the National Labor Relations Act." (GC Ex. 2 (2015 Policy) § 5.3.4; Tr. 96:5-20.) Additionally, to clarify that employees were permitted to discuss Section 7 protected subjects despite various restrictions within the policy pertaining to the protection of Confidential and Proprietary Information, revisions were made in 2015 to the definition of Confidential and Proprietary Information to make clear that "Confidential information does not include information about wages, hours, benefits and other terms and conditions of employment." (GC Ex. 2 (2015 Policy) § 4.2; Tr. 88:17-89:5.) Notably, the General Counsel takes no issue with these revisions to the policy. Nor does the General Counsel take issue with those provisions of the policy that allow the employer to review emails and monitor employee activity on the network. (GC Ex. 2 (2015 Policy) § 5.5; Tr. 97:4-98:19.)

Since 2008, the Electronic Asset Policy contained a section that allowed for employees to make incidental personal use of electronic assets, so long as the use was "incidental, limited in frequency and scope, cannot incur additional costs to KP, and cannot impact employee

performance." (Respondents' Ex. 1 (2008 Policy) § 5.4.1.2; Tr. 89:11-19.) In the 2015 revision, the policy added to this preexisting provision a definition of "Personal Use" as a defined term (as distinguished from "Working Time," which was also added as a defined term) and added the words "as defined in the policy" to the language of the Incidental Use Subsection. (GC Ex. 2 (2015 Policy) §§ 4.5, 4.6, 5.2.1; Tr. 89:6-19.) These changes clarify that the Incidental Use Subsection applied *only* to the "Personal Use" of electronic assets, as defined in the policy. The remaining language in the Incidental Use Subsection remained unchanged from its prior iteration.

Additionally, since 2008, the policy contained a prohibition on sending mass emails (i.e. to a large numbers of recipients) unless there was a clear business need to do so, although this did not strictly apply to the sending of mass "personal" emails. (Respondents' Ex. 1 (2008 Policy) § 5.2.4; Tr. 90:7-12.) In the 2015 revision, to comply with *Purple Communications,* the Mass Personal Messages Subsection was moved from the "Prohibited Use" section to the "Personal Use" section, and the language of the provision was modified to add the word "personal" and make explicit that the prohibition on the sending of mass emails now was limited to a prohibition against sending mass "personal messages." (GC Ex. 2 (2015 Policy) § 5.2.2; Tr. 90:7-91:18.) These changes made clear that the Mass Personal Messages Subsection applied only to "Personal Use" of electronic assets.

4. The Personal Use Section is entirely lawful even under a *Purple Communications* majority position

a) The Incidental Use Subsection allows limited use of Kaiser's email system for personal reasons and is permitted under *Purple Communications*

Putting aside that the General Counsel has not shown how the Incidental Use Subsection could reasonably be read as infringing on employees' exercise of their Section 7 rights (as it applies only to "Personal Use" of the employer's email system), the majority's decision in *Purple Communications* allows for this very type of restriction. In *Purple Communications*, the Board analyzed a policy that prohibited all personal use of the employer's equipment. *See* 361

NLRB No. 126 at 3 (policy states that "[a]ll such equipment and access should be used for business purposes only"). The Board further stated that an employer "may apply uniform and consistently enforced controls over its email system to the extent such controls are necessary to maintain production and discipline." *Id.* at 1. The Incidental Use Subsection here does not impose a total ban, but allows employees to use Kaiser electronic assets for personal reasons. Its only requirement is that such use be "incidental, limited in frequency and scope, cannot incur additional costs to KP, and cannot impact employee performance." (*See* GC. Ex. 2 (2015 Policy) § 5.2.1.) By its express terms, the policy is intended to limit use of Kaiser's email such that employee performance is not affected. Such a restriction is permitted under *Purple Communications* as a means to maintain production and discipline. *See* 361 NLRB No. 126 at 1.

In addition to maintaining production and discipline, the Incidental Use Subsection is necessary to secure Kaiser's network system. Email is the most prevalent vector that attackers use to infiltrate an organization's network. Emails sent by individuals outside Kaiser are also more likely to contain viruses, ransomware, and other types of malware. (Tr. 129:3-5.) Of the more than 200 million messages that Kaiser receives each month from external sources, approximately 85% of those messages must be discarded because they contain malicious content. (Tr. 130:11-16.) Unlike external emails, however, internal emails are considered "trusted" and are not subject to the same types of controls as external emails. (Tr. 134:6-16.) Thus, when an employee receives an email from an external source and forwards it on to another Kaiser employee, the risk of a breach is magnified because the external email has been reclassified as an internal email from a Kaiser employee. (Tr. 134:6-16.) It is now considered trusted and not scanned for malware as is protocol for external emails. (*Id.*)

Scanning and filtering through external emails is not enough to protect Kaiser's email system where hackers have become incredibly creative in bypassing the security controls. Although Kaiser has in place a system that filters and rejects up to 170 million external emails each month, it nevertheless finds that attackers are constantly evading its systems. (Tr. 152:24-153:8.) Internal limitations and restrictions are therefore necessary because an external email

with malware poses an even greater risk once it is forwarded within Kaiser's network as an internal email. It is not feasible to subject internal emails to same controls as external emails. Given the sheer volume of emails sent internally each day, the cost of scanning all such emails is prohibitively high. Kaiser would need to purchase technology from other vendors to review and scrub all these emails of malware. (Tr. 134:19-135:13.) Second, filtering internal emails would slow Kaiser's network and delay email delivery. (Tr. 135:20-136:5.) Because the internal email would need to be scanned and scrubbed of malware, employees would be delayed in receiving emails, which would further impact Kaiser's operations. (Tr. 135:25-136:5.)

Thus, in limiting employees' *personal* use of Kaiser's email systems to incidental usage only, the Incidental Use Subsection reduces the risk of a system breach that is attendant with employees forwarding external emails to other Kaiser employees. Without these measures in place, the integrity and security of Kaiser's electronic communication systems would be jeopardized. Moreover, if there is any confusion as to the scope of the Incidental Use Subsection, the remaining policies within the Electronic Asset Policy make clear that its restrictions do not apply to Section 7 activity. As an example, subsection 5.3.8 of the policy directly addresses Section 7 communication and provides that, although an employee may not use Kaiser's email system to solicit or proselytize for commercial ventures, religious causes, political candidates or parties, or outside organizations, the "provision does not apply to communications made by employees during non-working time that are protected under Section 7 of the National Labor Relations Act." (GC Ex. 2 § 5.3.8.)

b) The Mass Personal Messages Subsection complies with *Purple Communications*

As an initial matter, the *Purple Communications* majority did not create a right to distribute "mass email" or extend the Act's protections to activities that may jeopardize the security or efficient operation of an employer's computer systems. *C.f.* 361 NLRB No. 126 at 14. The Mass Personal Messages Subsection here limits the number of recipients per message to 500 because Kaiser's email system is specifically configured to allow individual emails to no

more than 500 recipients. It is built into the email system functions such that ***no one*** is allowed to send an individual email to more than 500 recipients. (Tr. 137:24-25.) This control is uniform and consistently enforced and is necessary to maintain production and network security. *See Purple Communications*, 361 NLRB No. 126, at 14 ("[W]e do not prevent an employer from establishing uniform and consistently enforced restrictions, such as prohibiting large attachments or audio/video segments, if the employer can demonstrate that they would interfere with the email system's efficient functioning.") Because the email cap applies to all messages sent on Kaiser's network, it is content neutral and does not distinguish between mass personal emails or mass emails sent for Section 7 purposes. The email cap ensures that the network runs smoothly, as the mere act of sending an email to hundreds of users causes a significant performance hit on the email systems. (Tr. 137:9-138:10.) Mass emails with large attachments can cause further disruptions by overloading the exchange server and delaying messages sent or received. Moreover, Kaiser's obligation under HIPAA to safeguard PHI mandates some controls over its email systems. Where PHI is inadvertently sent in a mass email to hundreds of recipients, Kaiser's ability to recall these messages and terminate improper access to PHI is significantly hampered. In the past, Kaiser information technology administrators have had to go to individuals directly to stop the spread of mass emails and direct them not to reply all to the mass emails. (Tr. 162:22-25.) The system's built-in cap of 500 recipients per email is thus necessary to ensure the protection of PHI, maintain network security, and prevent slowdowns in the network system.

Furthermore, the context provided by the Mass Personal Messages Subsection belies any claim that a reasonable employee would construe the terms such as "personal mass mailings," "chain letters," or "jokes" as reasonably encompassing Section 7 communications between employees. Because the Electronic Asset Policy encompasses numerous, related policies, it is necessarily contextualized and informed by rules contained elsewhere in the Electronic Asset Policy. *See Lutheran Heritage*, 343 NLRB at 647 (holding that the Board "must refrain from reading particular phrases in isolation, and it must not presume improper interference with

employee rights"). Policy no. 4.5 defines "Personal Use" as the use of emails "for personal reasons that do not relate to an employee's work for [Kaiser] or other issues relating to [Kaiser]." (GC Ex. 2 § 4.5.) Moreover, Policy no. 5.3.8 provides that while an employee may not use Kaiser's email system to solicit or proselytize for commercial ventures, religious causes, political candidates or parties, or outside organizations, the "provision does not apply to communications made by employees during non-working time that are protected under Section 7 of the National Labor Relations Act." (GC Ex. 2 § 5.3.8.) Indeed Kaiser specifically revised its Electronic Asset Policy after the Board's decision in *Purple Communications* to comply with the majority's new rule. (Tr. 96:15-24; 110:18-22; 111:7-9.) Against this backdrop, a reasonable employee would construe the Mass Personal Messages Subsection's prohibition of "chain letters, jokes, or other personal mass mailings" as a legitimate protection of Kaiser's email system, and not a prohibition on discussions of terms and conditions of employment.

The Mass Personal Messages Subsection also serves as guidance to Kaiser's managers regarding the approval of employee use of the network system to send emails to more than 500 recipients. Specifically, the policy provides that an employee may send authorized messages to large numbers of recipients with permission by the appropriate Kaiser manager. However, because Kaiser's email system is programmed to automatically reject any email to more than 500 recipients, practically the provision would only be triggered when and if an employee were to request permission to send an email to more than 500 recipients. (Tr. 136:16-25.) As a workaround to the software limitation, the employee would need to contact their manager for approval to create a distribution list of email addresses. (Tr. 137:1-7.) Not all employees are authorized to set up distribution lists, and administrators create such lists only upon proper request. (Tr. 137:4-7; 145:19-23.) The controls built into Kaiser's email system thus mandates that an employee obtain manager approval prior to sending an email to more than 500 recipients; the system does not allow the employee to send out mass emails otherwise.

In accordance with the policy, a manager may decline to approve an employee's mass email that serves no business purpose and which is purely personal in nature. Conversely, the

policy allows a manager to approve an employee's mass email where it relates to Kaiser's business or Section 7 purposes, so long as other requirements are met (for example, that any attachment to the mass email meets the maximum email size limit). There is no evidence in the record, nor does the General Counsel contend, that Kaiser has denied any employee request to email large numbers of recipients for Section 7 purposes or otherwise. Instead, the General Counsel is litigating a hypothetical situation here, as there has been so such employee request for authorization to send a mass email.

It should be additionally noted that the propriety of Respondents' rules against mass emails was previously reviewed by the Division of Advice in 2009. In a pre-*Purple Communications* decision, the Division of Advice nevertheless made an explicit approval of Respondents' mass email and incidental personal use rules, the language of which was the model for the language of the current provisions at issue in this case. Indeed, in its opinion, the Division of Advice expressly stated that "employer rules against mass emails strike a balance between employees' Section 7 rights and the Employer's legitimate business interest in ensuring the proper functioning of its email system." Although this finding was made by the Division of Advice based on the prior precedent of *Register Guard,* this finding is not inconsistent with *Purple Communications*' acknowledgement that employers may "apply uniform and consistently enforced controls over their email systems to the extent that such controls are necessary to maintain production and discipline." 361 NLRB at *14. Respondents reasonably relied on the Division of Advice's own analysis in deciding how to revise its Policy to comply with *Purple Communications*.

5. The Board should reverse *Purple Communications*

Notwithstanding the fact that the policy here complies with *Purple Communications*, the Board can and should use this case as the vehicle to reverse *Purple Communications* and to affirm *Register-Guard*, which embodies the Agency's historical position on the use of employer email for non-business purposes.

Purple Communications contravenes decades of Board precedent recognizing that employers are not required to allow employees to use employer-owned property for Section 7 purposes, as long as such restrictions are not discriminatory. *See, e.g., Mid-Mountain Foods, Inc.*, 332 NLRB 229, 230 (2000) (no statutory right to use employer's television); *Eaton Techs., Inc.*, 322 NLRB 848, 853 (1997) (no statutory right to use bulletin board); *Champion Int'l Corp.*, 303 NLRB 102, 109 (1991) (no statutory right to use copy machines); *Churchill's Supermarkets, Inc.*, 285 NLRB 138, 155 (1987) (no statutory right to use company telephones). A nondiscriminatory rule limiting use of an employer's email system to business purposes does not constitute and has never constituted interference with, restraint, or coercion of Section 7 rights. To the contrary, the Act "protects organizational rights," not the "particular means by which employees may seek to communicate." *Guardian Indus. Corp. v. NLRB*, 49 F.3d 317, 318 (7th Cir. 1995). Thus, while the Act prevents employers from discriminating against unions, it does not require employers to provide unions with the means, tools, or supplies to communicate their messages:

> Just as the right of free speech and association in the political marketplace does not imply that the government must subsidize political parties by distributing their literature without charge or giving them billboards on public buildings, so the right of labor organization does not imply that the employer must promote unions by giving them special access to [communications facilities].

Id. (citing *NLRB v. Honeywell, Inc.*, 722 F.2d 405, 406 (8th Cir. 1983) and *Container Corp.*, 244 NLRB 318, 318 n.2 (1979)).

For health care institutions such as Kaiser, an email system is, at its core, a means of communication to enhance patient care by streamlining communications between employees. (Tr. 95:14-21.) It represents a substantial business investment that includes not only includes the basic costs of networks, servers, and equipment, but also the costs of hundreds of support staff to maintain and update those systems – including the cost of ensuring the security of those systems from persistent threats of hacking and other security breaches designed to compromise the private information of patients and employees. (Tr. 135:4-17; 154:20-25; 176:8-178:4.)

Companies are and should be entitled to protect these investments by limiting their systems' use, in a non-discriminatory fashion, to the business purpose for which they are maintained.

The contrary conclusion by the *Purple Communications* majority is unsupportable for multiple reasons. First, there have been significant societal changes since the majority decided *Purple Communications*, including data breaches that affect both private companies and the government alike. Health care institutions like Kaiser are the most popular targets because they collect and store substantial amounts of PHI. If breached, attackers can access some of the most sought after and valuable information, such as social security numbers and medical information, to sell on the internet. (Tr. 139:20-140:1.) Not only are employees' and patients' information at risk, but prior data breaches have effectively shut down hospitals pending a ransom payment to the hackers to return the hospitals' network to working order. (Tr. 142:10-16.) In *Purple Communications*, the majority created a new presumption that employees who otherwise have access to an employer's email system may use that system for Section 7 communications during non-working time to "make national labor policy…responsive to the enormous technological changes that are taking place in our society." 361 NLRB No. 126 at 17 (quotation and citation omitted). Since *Purple Communications* was first decided, the quick pace of technology means that data breaches have not only grown in frequency but in their sophistication. The Board should respond to these real and increasing threats of data breaches and allow employers such as Kaiser the autonomy to control and protect their email systems and the privacy and protected health information of its patients and employees.

Second, *Purple Communications* was analyzed in the context of a relatively small shop – although the employer maintained call center facilities across the United States, only two call center facilities located in California were at issue in the litigation. The employer in *Purple Communications* was a company that provided specific services for deaf and hard of hearing individuals. In the facilities at issue in that case, it employed a total of only 77 employees. Kaiser, on the other hand, is one of the largest health care organizations in the world, with nearly 200,000 employees. Unlike the employer in *Purple Communications*, Kaiser collects and stores

PHI for hundreds of thousands of employees and roughly 11.8 million members in its system networks. Kaiser is not only obligated to protect PHI under HIPAA, but it is also constantly under attack by hackers seeking access to this enormous trove of information. Of the more than 200 million messages that Kaiser receives every month from external sources, 85-90% of those messages are discarded because they contain malware. (Tr. 120:11-13; 130:13-16.) The Board in *Purple Communications* did not need to consider issues such as the heightened cyber security vulnerabilities facing healthcare institutions such as Kaiser, the statutory obligation of maintaining PHI or even the now systematic attacks undertaken daily on healthcare providers such as Kaiser. The consequences are dire where healthcare institutions are breached; not only is PHI stolen and sold on the internet, but patient care is severely impacted as hospitals must cease operations until it pays a ransom to the hackers to release its network system. (Tr. 139:20-140:1; 142:10-24.) Hospitals such as MedStar, Hollywood Presbyterian, and the National Health Services in the United Kingdom are just a handful that have fell victim to these attacks. (Tr. 142:10-24.) The majority's holding in *Purple Communications* did not consider any of these issues and is therefore inapposite here.

In sum, Respondents request that the Board reverse its decision in *Purple Communications*, and reaffirm, consistent with decades of precedent, that employees do not have a statutory right to use their employer's email for Section 7 purposes.[13]

D. The Recording Section Does Not Violate The Act

1. The Recording Section is Lawful Under the Board's Current Standards

The ALJ should reject the General Counsel's challenge to Respondents' policy provision governing recording in its workplace for the simple and compelling reason that it is lawful under binding Board precedent. The Recording Section of Respondents' Electronic Asset Policy complies with the Board's current standards as articulated in *Whole Foods Market, Inc.*, 363

[13] Moreover, if the Board intends to impose a new burden such as this on employers, it should do so via rulemaking rather than through adjudication.

NLRB No. 87 (2015) ("*Whole Foods*"), *approved at* 691 Fed.Appx. 49 (Mem) (2d. Cir. 2017), and *Flagstaff Medical Center*, 357 NLRB No. 65 (2011) ("*Flagstaff*").

In *Flagstaff*, the Board analyzed whether a hospital employer's portable electronic equipment policy, which broadly prohibited "the use of cameras for recording images of patients and/or hospital equipment, property, or facilities," violated Section 7. 357 NLRB at *6. In holding that the rule did not violate Section 7,[14] the Board found that the "privacy interests of hospital patients are weighty, and [the hospital employer] has a significant interest in preventing the wrongful disclosure of individually identifiable health information, including by unauthorized photography." *Id.* The Board concluded that employees would reasonably interpret the rule as a legitimate means of protecting the privacy of patients and their hospital surroundings, not as a prohibition of protected activity, and thus determined that there was no Section 7 violation. *Id.*

In *Whole Foods*, the Board found that a similar no-recording policy in a retail grocery setting to be unlawful. 363 NLRB No. 87, at *4. However, in *Whole Foods,* the Board expressly distinguished its holding from its prior decision in *Flagstaff*, which upheld a similar no-recording policy in a hospital setting. *Id.* In reconciling the two decisions, the Board acknowledged that audio or video recording in the workplace is only protected by Section 7 under *certain circumstances*[15] – i.e. when employee are acting in concert for their mutual aid and protection and no overriding employer interest is present. *Id.* at *3. In a hospital setting, as opposed to a retail grocery setting, the "weighty patient privacy interests and the employer's well-understood HIPAA obligation to prevent the wrongful disclosure of individually identifiable health information," are so "pervasive and compelling" as to warrant prohibitions

[14] The Board also noted that, as is true here, the *Flagstaff* employer's no-recording rule did not expressly restrict Section 7 activity, was not promulgated in response to Section 7 activity, and was not applied by the employer to prohibit Section 7 activity. *Id.*

[15] As the Second Circuit concedes, not every no-recording policy will infringe on employees' Section 7 rights. *Whole Foods Mkt. Grp., Inc. v. NLRB,* 691 F. App'x at 51, n.1 (*citing Flagstaff,* 357 NLRB at 659-60 for the holding that a no recording policy was lawful "where hospital demonstrated patient privacy interest.").

against recording that might otherwise be unlawful. *Id.* at *4 (2015) (citing *Flagstaff Medical Center,* 357 NLRB No. 65 (2011)). *Flagstaff* therefore remains good law, preserving an **exception** for no-recording policies in a healthcare setting.

As the most recent expression of Board law concerning no-recording policies, the ALJ is required to follow the Board's decision in *Whole Foods* and *Flagstaff* (as it relates to recording policies in a hospital setting), absent a strong reason to conclude that the Board would rule differently. *See Ford Motor Co. (Chicago Stamping Plant) v. NLRB*, 571 F.2d 993, 996 (7th Cir. 1978) ("The Board takes the view that an Administrative Law Judge's duty is to apply established Board precedent which the Supreme Court of the United States or the Board itself has not reversed"). Here, the General Counsel presented no evidence that would distinguish *Flagstaff* from the instant case or that would give the ALJ any reason to conclude that the Board would rule differently in this case than it has in *Flagstaff.* In this context, the General Counsel's case is nothing more than a bare invitation to the ALJ to overrule (or simply ignore) *Flagstaff.* But the ALJ is bound to follow Board precedent – in this case precedent re-affirmed by the Board as recently as 2015.

Like the policy in *Flagstaff*, Respondents enacted the Recording Section of the Electronic Asset Policy to protect its patients' privacy interests and adhere to its HIPAA obligation to prevent the wrongful disclosure of individually identifiable health information. These are pervasive and compelling interests that the Board has found to justify a rule's restrictions on Section 7 activity. *See Flagstaff*, 357 NLRB at *6 ("The privacy interests of patients are weighty"); *Whole Foods*, 363 NLRB at *4 (recognizing that patient privacy interests and obligation to protect PHI are "pervasive" and "compelling"). The undisputed evidence in this case plainly shows that the Recording Section is lawful under well-established – and current – Board law.

2. The Recording Section is Necessary to Comply with HIPAA Regulations

As healthcare providers, hospitals and medical insurance providers, Kaiser is required to comply with HIPAA, 42 U.S.C. §§ 1320d-6 &1320d-9, the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, and any and all other Federal regulations and interpretive guidelines. (See Respondents' Ex. 7 (Request for Judicial Notice) and Exs. 7(M-P); Tr. 167:13-24.) HIPAA specifically protects the privacy of and prohibits the unauthorized disclosure of PHI. (Tr. 183:3-10.) To comply with HIPAA, Kaiser is required to take broad steps to maintain the confidentiality of PHI and restrict the use and disclosure of PHI.

The risk of inadvertent disclosure of PHI is significant at Kaiser because PHI is present throughout Kaiser's premises. PHI includes any information related to individuals, their health, and their health insurance. (Tr. 170:3-9.) It is not limited to medical information, but encompasses identifying marks on an individual, such as a birth mark or tattoo. (Tr. 170:22-171:1; 171:4-9.) It is important to understand that the presence of PHI in a health care facility is not limited to so-called "immediate patient care areas," as that term has been used in Board law. PHI is located throughout the hospital setting; it is the patients themselves, what can observed of the patients (e.g., whether they are on a gurney or intubated), discussions by caregivers about the patient, and information posted on walls about the patient (e.g., hospital charts or operating room schedules). (Tr. 171:17-25; 195:19-24; 196:2-10.)

Kaiser is legally bound to protect all such PHI under HIPAA, and is subject to fines and penalties for any violation. (Tr. 173:14-19.) Kaiser's obligation to protect PHI is also rooted in its contractual requirements with entities that purchase its health insurance, including employer groups that purchase insurance for its employees and governmental purchasers that provide coverage through Medicare, Medi-Cal, and state employee programs. (Tr. 173:1-6.) These contracts also impose penalties for violations. (Tr. 173:14-19.) In addition to fines, the Joint Commission for Healthcare Organizations and the National Committee on Quality Assurance

may revoke Kaiser's accreditation or license for breaching its duty to safeguard PHI. (Tr. 174:1-7.)

The Recording Policy is therefore necessary to facilitate Kaiser's compliance with HIPAA. Inherent in Kaiser's business as healthcare providers is the risk of disclosure of protected health information in the event that surreptitious recording was allowed to take place at Kaiser facilities (i.e. hospitals, medical offices, and medical administrative facilities) of Kaiser personnel, health plan members, patients, or their family. Given the breadth of PHI throughout the workplaces, the risk of inadvertently capturing such information by making recordings on Kaiser premises is substantial. (Tr. 179:14-18.) A video recording at the hospital may capture patients on their hospital beds; medical charts showing the patient's name, medical record numbers, diagnoses, medications, and other medical history; and even conversations amongst medical professionals as to the condition of certain patients. (*See* Tr. 178:13-16.) Indeed, and importantly, even a photo taken in a Kaiser cafeteria or parking lot could include PHI if a patient seeking medical treatment was inadvertently captured. (Tr. 195:19-196:12.) The Recording Section of the Electronic Asset Policy therefore prohibits the making of audio, digital or video recordings on Kaiser premises or of Kaiser personnel, patients, or their family members without the consent and authorization of all who are being recorded. (GC Ex. 2 (2015 Policy) § 5.3.8.) Consent of those being recorded is necessary to avoid HIPAA violations. (Tr. 202:3-15.)

3. The Recording Section is Necessary to Comply with California and Other State Statutes Prohibiting Unauthorized Recording Without Consent

Kaiser's obligations to maintain patient privacy arises, not only under HIPAA, but also under the laws of various states in which Kaiser operates. Indeed, the vast majority of states in which Kaiser operates are "two-party consent" states that prohibit the recording of **any** communication without the consent of all parties to the conversation. California, Washington, Maryland, and Georgia require that all parties consent to the recording of a communication and impose fines or imprisonment for violations. *See* Cal. Penal Code § 632 ("A person who,

intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication" shall be punished by a fine and/or imprisonment); Rev. Code Wash. § 9.73.030 (it shall be unlawful "to record any...[p]rivate communication, by any device electronic or otherwise designed to record or transmit such conversation...without first obtaining the consent of all persons engaged in the conversation"); Md. Courts and Judicial Proceedings Code § 10-402; Code of Georgia § 16-11-62 ("It shall be unlawful for...[a]ny person, through the use of any device, without the consent of all persons observed, to observe, photograph, or record the activities of another which occur in any private place and out of public view").[16] These state regulations demand that Respondents maintain the Recording Section.[17] Thus, in addition to Kaiser's HIPAA obligations, the Recording Section of the Electronic Asset Policy is also designed to comply with two party consent statutes in California and other states and accordingly does not impose any restriction on recording where there is "consent and authorization of all who are being recorded." (Tr. 82:12-15.) [18]

In *Whole Foods,* the Board briefly noted, and summarily dismissed, the employer's argument that it operates in many states where nonconsensual recording is unlawful. 363 NLRB No. 87, n. 13. However, *Whole Foods* was not concerned with the weighty privacy interests of patients in a hospital setting. As *Flagstaff* counsels, healthcare institutions are different than other employers in that the employer is tasked with maintaining not only the privacy of

---

[16] The ALJ took judicial notice of the state recording statutes for each state in which Respondents operate. (*See* Respondents' Ex. 7 (Request for Judicial Notice) and Exs. 7(E-L).)

[17] It cannot be the Board's intent to undermine employers' efforts to adhere to long-established state laws. To do so would place employers in the untenable situation of running afoul of state law in order to comply with the Board's reading of the Act. To the extent that *Whole Foods* considered and dismissed – as an employer's justification for a no-recording policy – compliance with state privacy laws in a healthcare setting (which is did not), *Whole Foods* was wrongfully decided on this point.

[18] Kaiser's duty to adhere to "two-party consent" for recordings is especially pressing here, where its operations are primarily located in California. (Tr. 82:12-15.) In fact, two Kaiser entities, TMPG (the only proper party subject to a timely charge) and SCPMG, operate ***exclusively*** in California and do not treat any patients or employ any individuals outside the state. (Tr. 62:2-10; 113:5-10.) Therefore, unlike in prior Board decisions evaluating privacy considerations, the majority of affected employees – as well as the majority of affected patients – are based in California, and Kaiser therefore has a stronger interest in complying with California law.

employees, but also the confidentiality of third party patients' protected health and medical information. *Flagstaff*, 357 NLRB at 663. When the business justification of the policy is the employer's protection of a patient's right to the privacy of their medical information, *Flagstaff* and *Whole Foods* stands for the proposition that employees' limited right to make recordings must yield. Accordingly, Kaiser's compliance with two party consent statutes provides further justification for the language and restrictions of the Recording Section of the Electronic Asset Policy.

4. Patient Privacy Interests Not Present In *Whole Foods* Justifies The Recording Policy Here

Flagstaff and *Whole Foods* recognize that patient privacy interests are so pervasive and compelling as to warrant some restriction on an employee's ability to make recordings in the workplace. Healthcare workplaces are plainly distinguishable from other workplaces because healthcare workplaces are in the business of dealing with protected health information. *Whole Foods,* 363 NLRB at *4 (the significant HIPAA privacy considerations that rendered a similar no-recording policy violation-free in *Flagstaff* did not apply to Whole Foods because Whole Foods was not in the business of dealing with protected health information).

Given these risks and the operational differences between a hospital and a grocery employer, the Board would not be justified in arriving at an outcome like *Whole Foods* in this case. The Board cannot simply ignore Kaiser's far greater interest in complying with HIPAA and safeguarding its patients' confidential medical information. Unlike the employer in *Whole Foods*, Kaiser is concerned not only with the privacy interests of its employees, but also with the privacy interests of its patients which *Flagstaff* and *Whole Foods* counsels must be given special consideration. Patient privacy interests are plainly distinguishable from other business justifications. Indeed, an ALJ who was recently called upon to evaluate a telephone company's no-recording policy recently held:

> A medical condition is among the most personal pieces of information an individual possesses. The disclosure of such sensitive information to anyone is a choice only that person should be making. The recording of a

> patient being treated with a certain type of hospital equipment or residing in a particular wing of a hospital plainly could permit others to determine the person's medical conditions. [By contrast, a] customer's number of phone lines, the services and features of their phone service, and their phone usage cannot plausibly be said to rise to the same level of sensitivity as individually identifiable health information. Even though an individual's social security number, date of birth, credit card information, and authentication credentials are of greater sensitivity, they remain pieces of information that are not as weighty as a medical condition. A credit card can be reissued, a password can be reset, and an individual's identity can be protected in any number of ways after disclosure of a social security number and birth date. The same cannot be said after a medical condition has become public.

Michigan Bell Tel. Co. & AT&T Servs., Inc. (Local 4034, Commc'ns Workers of Am., AFL-CIO), Case No. 07-CA-182505, 2017 WL 4334532 (Sept. 27, 2017). In *Flagstaff*, the Board pronounced that a no-recording policy is valid in a healthcare setting to protect these weighty patient privacy interests. *Flagstaff,* 357 NLRB at *6. As the most recent pronouncement of Board law concerning recording policies in the healthcare setting, the Board here must adhere to *Flagstaff* and *Whole Foods* and find that Kaiser's Recording Section is lawful

V. CONCLUSION

For the foregoing reasons, Respondents respectfully request that the Board dismiss the Complaint in its entirety.

DATED: November 7, 2017

Respectfully submitted,

By:

MICHAEL LINDSAY
mlindsay@nixonpeabody.com
ALICIA ANDERSON
acanderson@nixonpeabody.com
MAE K. HAU
mhau@nixonpeabody.com
NIXON PEABODY LLP
300 South Grand Ave., Suite 4100
Los Angeles, California 90071-3151

Attorneys for Respondents, KAISER FOUNDATION HEALTH PLAN, INC., KAISER FOUNDATION HOSPITALS, and SOUTHERN CALIFORNIA PERMANENTE MEDICAL GROUP

PROOF OF SERVICE

I, the undersigned, certify that I am employed in the City and County of Los Angeles, California; that I am over the age of eighteen years and not a party to the within action; and that my business address is 300 South Grand Avenue, Suite 4100, Los Angeles, California 90071. On November 7, 2017, I served the following document(s):

RESPONDENTS' POST-HEARING BRIEF

on the parties stated below, through their attorneys of record, by placing true copies thereof in sealed envelopes addressed as shown below by the following means of service:

___: By First-Class Mail — I am readily familiar with the firm's practice for collection and processing of correspondence for mailing. Under that practice, the correspondence is deposited with the United States Postal Service on the same day as collected, with first-class postage thereon fully prepaid, in Los Angeles, California, for mailing to the office of the addressee following ordinary business practices.

____: By Overnight Courier — I caused each such envelope to be given to an overnight mail service at Los Angeles, California, to be hand delivered to the office of the addressee on the next business day.

__XX__:By Email or Electronic Transmission— By electronically mailing a true and correct copy through Nixon Peabody's electronic mail system from mdelgadillo@nixonpeabody.com to the addresses set forth below.

Danielle Lucido Email: dlucido@ifpte20.org	**Attorneys for Petitioner Engineers and Scientists of California, IFPTE Local 20, AFL-CIO & CLC**
Judy Chang Email: judy.chang@nlrb.gov	**Field Attorney** **National Labor Relations Board, Region 32**

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 7, 2017, at Los Angeles, California.

Mayra Delgadillo